Submission in Response to NSF CI 2030 Request for Information

DATE AND TIME: 2017-04-05 15:48:40
REFERENCE NO: 266

Author Names & Affiliations

- David Dampier - Mississippi State University
- Kari Babski-Reeves - Mississippi State University

Contact Email Address (for NSF use only)

(Hidden)

Research Domain, discipline, and sub-discipline

cybersecurity

Title of Submission

Cybersecurity and infrastructer--Control Systems and IoT

Abstract (maximum ~200 words).

As more and more systems become designed for remote access and control, the Internet of Things (IoT) will have a profound impact on how systems are designed and managed. Additionally, modification of current closed-loop systems to allow for remote access has introduced pathways for attacks that need to be addressed holistically. This submission identifies challenges associated with the IoT and control systems used to monitor and control IoT devices and computing needs. Further, ass a result of increased connectivity, there is a reciprocal increasing reliance on advanced cyberinfrastructure for the advancement of science and engineering research across all disciplines is straining both campus and national CI resources. Over the next decade the demand for computational cycles, storage capacity, and network bandwidth will likely increase by multiple orders of magnitude. Additionally the demand for trained cyber practitioners (systems administrators, data managers, domain-specific consultants, etc.) will grow at an equally high rate. Without sufficient planning and development of novel approaches to address each of these needs, there will insufficient resources and capability to serve individuals, companies and organizations, and governments.

Question 1 Research Challenge(s) (maximum ~1200 words): Describe current or emerging science or engineering research challenge(s), providing context in terms of recent research activities and standing questions in the field.

New and emerging areas of research in this area include Internet of Things (IoT) and Control Systems. The IoT refers to all systems or devices (things) that are interconnected on the Internet. Devices; such as cell phones, tablets, laptops, etc.; are well known, and the methods for securing these devices are fairly well understood. Devices that are part of the IoT that are not as well understood include:
• vehicles (air, ground, water), either autonomous, semiautonomous or manual;
• household devices, such as appliances, lighting, smart door bells;

• security systems, such as security sensors, digital camera systems, smoke alarms, fire sensors;
• Supervisory Control and Data Acquisition (SCADA) Systems for critical infrastructures, like water systems, gas pipelines, power grid;
• control systems for manufacturing applications, like assembly line computers, power generation systems, flow control;
• cloud servers and data centers;
• and many others.
Security for these systems are not so well understood either because they are new and untested (such as for autonomous vehicles and household devices) or historical issues remain unsolved (such as for control systems). However, competing objectives (e.g., real-time assessment and decision making ability vs security protocols) remains as a historical and current issue that must be addressed in the near future to allow for radical changes in systems design, rather than incremental changes. Additionally, many systems were designed to run as closed systems but have been modified to allow for remote connectivity for monitoring and access by various users of these systems. Remote monitoring provides an attack vector that was not envisioned in the initial design of these systems, and as such the cyber security of these systems is an area of research that has been growing steadily for a number of years. As the world transitions more and more to the IoT systems, there is a critical research need for understanding the vulnerabilities of these systems, appropriate detection methodologies, mitigating protocols and system redesigns.

The following are some examples of current and past research projects that might provide some context for this problem area:
1) Electric Ship Research and Development Consortium (ESRDC)
Over the past 3 years the ESRDC has significantly advanced the knowledge base and developed competencies in all relevant areas of expertise pertaining to the design of electrical power and energy systems for future naval surface combatants. The Navy is moving forward with the concept of increasing the role of the electric power generation and distribution system in the effectiveness of combat mission loads. To be successful in that effort, several areas in the domain of design and analysis of Combat Power and Energy Systems (CPES) will need further development and refinement. Outside the Navy, the technology to support design of complex systems is being advanced globally. This research is important to help the Navy use appropriate approach(es) to achieve affordable superiority. The goal of this thrust is to advance the state of the art of the design and analysis methodologies for readiness to be implemented in the Smart Ship Systems Design (S3D) environment, the ESRDC's preferred design tool for agile and rapid design development. Development of the approaches in this tool-independent thrust before migrating them to the S3D thrust will ensure that the approaches are broadly applicable for any design process and independently tested.

On the application level, the availability of well designed and tested system level control approaches will be a prerequisite for a successful implementation of the CPES concept on future surface combatants. The recently announced Controls Future Naval Capability (FNC) program further illustrates the importance of controls in the design of CPES. On the technical level, the field of controls is undergoing rapid change. Recognizing the limitation imposed by communication latency, power system control approaches are focusing on coordinated local control to react to changes on the appropriate time scale. Control approaches are being developed that dynamically incorporate risk and changing priorities. Control hardware is becoming faster, more versatile, and more affordable. ESRDC has a long history of work in the field of systems level control. The objective of this thrust is to develop control algorithms and methods that provide a variety of capabilities and desired features, such as power and energy management, system state monitoring, system stability management, equipment health monitoring, fault management.

2) Enterprise System Security: Sponsor-Engineering Research and Development Center (ERDC)
Protecting research and development and infrastructure networks is a challenging task due to their complex and heterogeneous nature. Traditional protection systems have, to a large extent, only addressed the detection problem, leaving the defense steps to be performed manually by the system administrators. In this work MSU is attempting to build a holistic and autonomic Intrusion Detection and Response System, able to plan at run-time, defense strategies to reactively and proactively counter detected and predicted attacks, able to evolve according to the actual system and attacker behaviors and able to discover new attack patterns in order to be effective against 0-day attacks.

Anomaly detection and threats management are active research areas, but most of the works proposed so far have not considered the connection points between them. This separation had an impact on the available threat recognition software applications as well, because none of them consider the whole threat recognition and management chain, starting from monitoring, passing through an ensemble-based analysis of all the information flows and ending with the defense planning and execution. The holistic model-based Intrusion Detection and Response System for Research and Development and infrastructure networks that we are designing and developing in this project will be the first software able to provide a comprehensive protection to such critical infrastructures.

3) Power System Security: Sponsor-Department of Homeland Security
Resilient systems must detect attacks in order to provide an appropriate and rapid response. As such intrusion detection systems are a key

underlying requirement. Event and intrusion detection systems must be aware of the normal operating behaviors of the protected system to detect actions which will drive the system toward a critical state. Specification based intrusion detection systems feed measurements from physical and cyber components to model device behavior in real time. Intrusion detection systems must detect previously unknown attacks; also known as zero day attacks. Intrusion detection systems must be aware of known and possible cyber-attacks. Signature based intrusion detection system technology compares device behaviors to signatures of known attacks to provide a highly accurate attack detection mechanism. MSU researchers will continue research each of the three aforementioned intrusion detection areas.

Intrusion detection systems monitor network actions, host actions, and physical system actions. Monitoring technologies must be unobtrusive to allow the systems to operate without significant degradation from the monitoring sub-system. MSU researchers will extend research in high-performance application for scalability and reconfigurable computing to design active response system that detects the anomalies in real-time (or near real-time). High-performance application platform enables the design of application-specific processing elements that can operate in parallel, reducing detection latency, maximizing performance, and fast and scalable EIDS. An instance of EIDS consists of sensors data input, data processing and attribute selection component, event classifier algorithms, and a management system that manages alarm and alerts.

Question 2 Cyberinfrastructure Needed to Address the Research Challenge(s) (maximum ~1200 words): Describe any limitations or absence of existing cyberinfrastructure, and/or specific technical advancements in cyberinfrastructure (e.g. advanced computing, data infrastructure, software infrastructure, applications, networking, cybersecurity), that must be addressed to accomplish the identified research challenge(s).

The exponential growth in the number of IoT devices deployed will create vast opportunities for research activities, but with complex challenges to the cyber infrastructure. The connecting of everything to the Internet will create massive quantities of constant data streams, in many cases overwhelming the available network infrastructure. This never-ending inflow and outflow of data will not only stress capacities and performance of storage systems, but will also exceed existing data management strategies and technologies. Coupled with the simultaneous need for real-time analysis of this very same data, the computational resources will need to robust and plentiful. Therefore, research on resource sharing, protocols for distributed allocation of resources, hierarchical protocols for various systems, etc. are vastly needed to support efficient utilization of current and future infrastructure needs. Additionally, research on advanced cyberinfrastructure (materials, storage, power, etc.) is a critical need.

With a constantly increasing demand for advanced cyberinfrastructure, over the next decade many research institutions will struggle to provide the necessary level of advanced CI resources needed to support a growing user base spanning broader domains of science and engineering. Inevitably the most prominent researchers or those with the highest profile activities will be given priority to campus CI resources, with the remaining researchers left to fend for whatever resources are left. While the national-level resources can help to reduce campus contention, these national-level resources tend to be devoted to capability-class computing activities, and rightfully so. The campus environments need to have sufficient, locally-managed CI resources with the ability to define their own priorities and policies. These campus systems will be where the vast majority of the capacity-class computing activities should be conducted.

The challenges of the next decade don’t end with just computational, storage and networking infrastructure, but also include the need for a vibrant and creative workforce to support advanced cyber infrastructure. The demand for well-trained cyber practitioners, such as systems administrators, network engineers, domain-specific consultants and the many other necessary personnel supporting researcher activities, is at an all-time high today. With limited avenues for training the next generation of this critical CI workforce, the ability to significantly grow research activities involving ever more complex advanced CI is questionable over the next decade.

Consent Statement

- “I hereby agree to give the National Science Foundation (NSF) the right to use this information for the purposes stated above and to display it on a publically available website, consistent with the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode).”